

Department of Defense Common Access Card (CAC) Fact Sheet



Updated: January 2003

Description: The Department of Defense (Department or DoD) is implementing smart card technology as a Department-wide Common Access Card (CAC). A smart card is a credit card size token with one or more embedded memory and/or microprocessor integrated circuit chips (ICC). The CAC also contains a linear barcode, two-dimensional barcode, magnetic stripe, color digital photograph, and printed text. The CAC will be the standard identification card for active duty military personnel, Selected Reserve, DoD civilian employees, and eligible contractor personnel. The CAC will also be the principal card used to enable physical access to buildings and controlled spaces and for logical access to the Department's computer networks and systems. The CAC ICC has a cryptographic co-processor to enable it to serve as a token for the PKI identity, email, and encryption certificates.

Background: Since 1993, the DoD has been conducting evaluations on smart card technology. Initially tested as an updateable, individually carried data storage device, the Department's smart card mission has evolved to require an interoperable, backward compatible device for secure on-line data transfer and on-line transactions. Successful pilots and demonstrations in the late 1990s, resulted in the Department directing the use of smart card technology for multiple applications on a single platform, the Common Access Card.

General Characteristics

Primary Function: Smart card using multiple technologies to perform standard identification, physical access, and logical access for active duty military personnel, Selected Reserve, DoD civilian employees, and eligible contractor personnel.

Program Management: The DoD Access Card Office performs program management and execution responsibilities under the operational control of the DoD Chief Information Officer, and under the policy direction and oversight of the DoD Electronic Business Board of Directors and the Smart Card Senior Coordinating Group. The DoD Access Card Office falls under the cognizance of the Defense Manpower Data Center, which reports to the Office of the Under Secretary of Defense for Personnel and Readiness.

Applications: Mandatory applications for the CAC are identification, logical access and authentication using the CAC as the hardware token for the DoD-wide Public Key Infrastructure (PKI), and physical access. Other applications are designated as Department-wide or Component-specific. Department-wide applications currently under development and/or evaluation include food service, financial (stored value, ATM, electronic purse), and Joint exercises. Component-

Department of Defense Common Access Card (CAC) Fact Sheet



specific applications currently under development and/or evaluation include stored value, medical and dental readiness, student visibility, armory and property accountability, training, rifle range, and deployment readiness.

Infrastructure: Fielded infrastructures are being used in the deployment of the CAC. The existing infrastructure of the Defense Enrollment Eligibility Reporting System (DEERS) and Real-time Automated Personnel Identification System (RAPIDS) is being modified to integrate the multiple CAC applications and many of the functions of the Local Registration Authority (LRA) workstation.

Contractor: Multiple

Target Population: Approximately 4 million active duty military, Selected Reserve, DoD civilian employees, and eligible contractors by October 2003.

Unit Cost: Estimated at \$6 - \$10 per card (additional costs per seat for middleware and card readers will be required).

Dimensions: The CAC follows the International Standards Organization (ISO) 7816 series for integrated circuit cards for electrical contact. Its dimensions are credit card size (approximately 2.25" x 3.625").

CAC Technologies: An integrated circuit chip containing 32Kb of data storage and memory, a linear (Code 39) barcode, a two-dimensional (PDF 417) barcode, a magnetic stripe, and a color digital photograph. Multiple technologies exist on the CAC to accommodate the migration of multiple applications using a combination of existing barcode and magnetic stripe reader infrastructure to the new smart card ICC reader technology. The CAC is a commercially derived solution and follows commercial standards to the greatest extent possible.

Program Status: In October 2000, the Department of Defense began initial testing of the Department's implementation of smart card technology, the Common Access Card. Beta testing of the CAC completed with the issuance of 95,000 cards. Implementation DoD-wide commenced in November 2001. By October 2003, approximately four million cards will be issued worldwide.

Because of such a large and diverse cardholder population, a comprehensive communications strategy that encompasses both internal and external stakeholders is in full implementation. The purpose of the communications strategy is to plan for and facilitate changes as a result of the CAC implementation by organizing resources to create a uniform and consistent awareness of the CAC, its functions, and capabilities. The communications strategy will ensure that all cardholders and those who use the CAC for

Department of Defense Common Access Card (CAC) Fact Sheet



identification, access, and benefits are educated and knowledgeable on the CAC prior to full implementation.

Currently, additional capabilities and functionalities being tested include an additional chip (contactless – 14443A), 64Kb of memory, FIPS 140-2 level 3, and biometrics.

System Timeline: Beta Test – 1st Quarter FY 2001; Initial Operational Capability -- November 2001; Final Operational Capability – October 2003

Point of Contact:

DoD Access Card Office
Defense Manpower Data Center
1555 Wilson Blvd., Suite 609
Rosslyn, VA 22209
Phone: (703) 696-7396
Internet: <http://www.dmdc.osd.mil/smartcard>